KRYPTERING
- FORUDSÆTNINGEN FOR PRIVACY

INTERNETDAGEN 2019

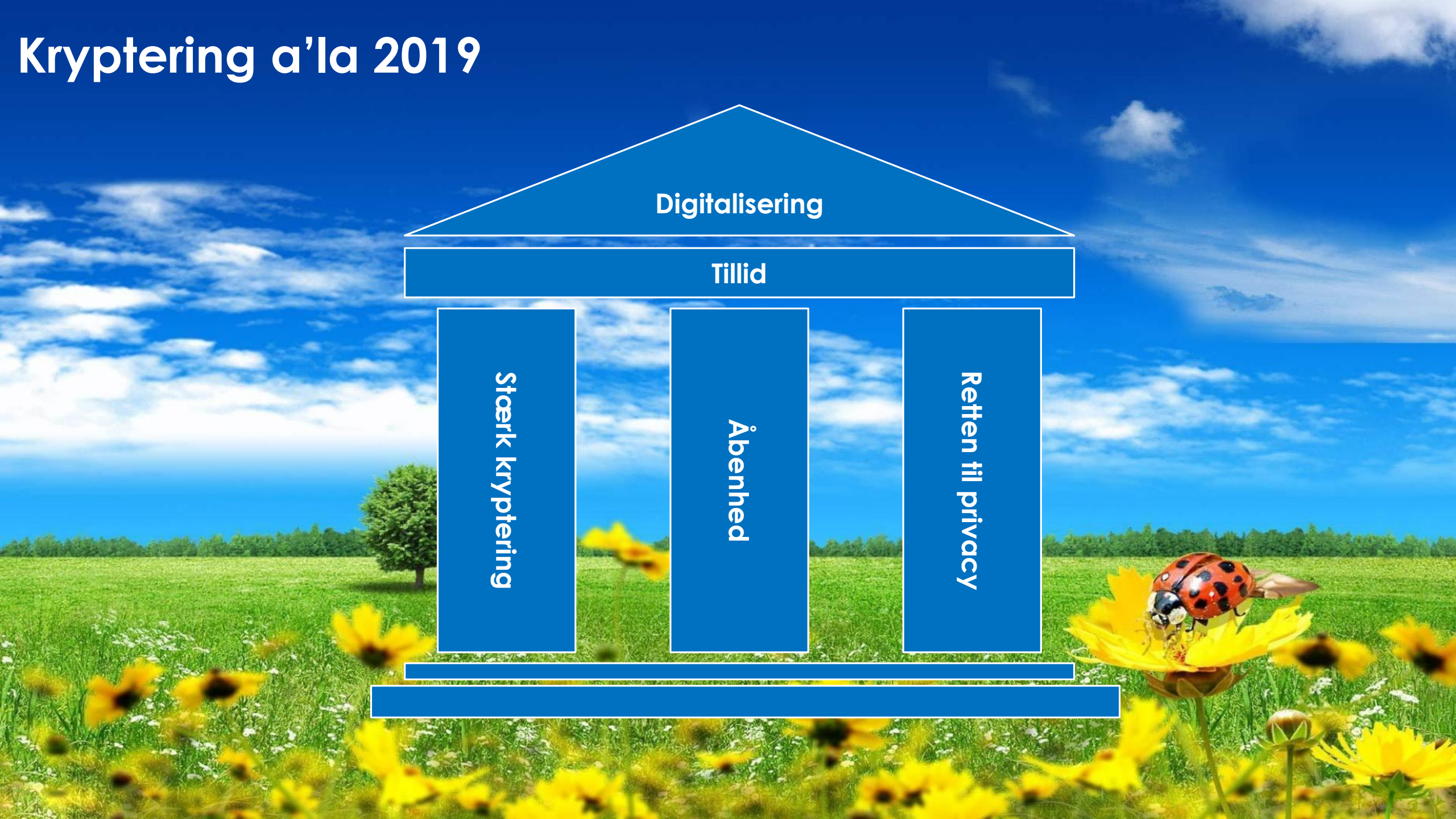
Søren Sennels, Dencrypt

TAKE AWAY:

Sikker kryptering er ikke en naturlov.

Pas på det!

Kryptering a'la 2019



3 fundamentale opdagelser

Vincent Rijmen
Joan Daemen

AES
(2001)

Symmetrisk kryptering
256-bit nøgle

Fundamentale opdagelser

Sikker nøgleudveksling

Diffie-Hellman
(1976)

Withfield Diffie
Martin Hellman

Asymmetrisk kryptering.
Digital signatur

RSA
(1977)

Ron Rivest
Adi Shamir
Leonard Adleman

Teknologisk trussel: Kvantecomputere

RSA: Heltals faktorisering

$n = p * q$

Diffie-Helman: Diskrete logaritme problem

$A = g^s \bmod p$

} Kompleksitet: 2^n

Peter Shor

1994: Shor's algoritme → Kompleksitet: n^x

RSA: Usikker

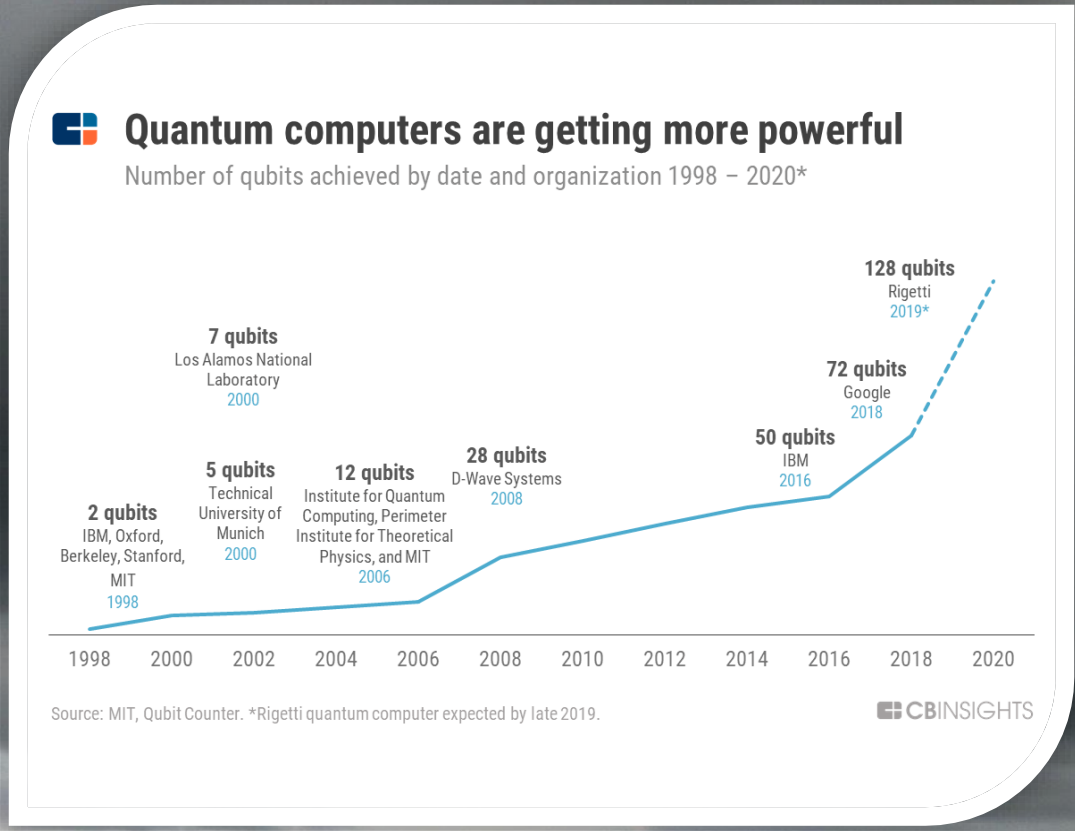
DH: Usikker

~4000 qubits til at bryde RSA2048

Lev Grover

1996: Grover's algoritme: Hurtig brute-force attack. Halverer effektive nøglelængde.

3DES:	$2^{168} \rightarrow 2^{84}$	Usikker
AES-128:	$2^{128} \rightarrow 2^{64}$	Usikker
AES-256:	$2^{256} \rightarrow 2^{128}$	Sikker



Politisk trussel: Udfordrer retten til privacy

1975: NIST introducerer Data Encryption Standard (DES).
Reducerede nøglelængden fra 128 til 56 bit.

1987: Indfører bevidst svage krypteringer i 2G/GSM standarden:
A5/1: Sikker (dengang!)
A5/2: Svækket, beregnet til eksport ud af Europa
A5/0: Ingen kryptering (French mode)

1993: NSA forsøger at indføre "key escrow" hos teleoperatørene.

2018: Australia introducerer ny krypteringslovgivning
Pålægger leverandører at give adgang til krypteret data.

Clipper chip

Search jobs | Sign in | Search | International edition

The Guardian

8. Juli 2019

Australia's anti-encryption laws being used to bypass journalist protections, expert says

New legislation has given AFP 'power to strike a chilling blow against press freedom', cybersecurity researcher tells parliamentary review

Faktum:
Alle har idag adgang til sikre krypteringsløsninger.

Relevante spørgsmål:

Er indskrænkningen af retten til privacy berettiget?

Giver det reelt højere opklaringsrater?

Giver det reelt bedre efterretninger?

Kunne disse opnås med andre midler?